

Оглавление

| | |
|---|-----------|
| Введение..... | 3 |
| 1. Анализ текущего состояния | 11 |
| 1.1. Описание технологии и типовой архитектуры системы квантового распределения ключей | 11 |
| 1.2. Анализ известных способов преодоления максимальной дальности создания квантовых ключей . | 18 |
| 1.2.1. Анализ структуры сети КРК по версии ETSI | 24 |
| 1.2.2. Анализ структуры сети КРК по версии ITU-T.... | 29 |
| 2. Особенности применения технологии квантового распределения ключей для сегмента сети в топологии точка-точка | 40 |
| 2.1. Способ построения классического аутентифицированного канала квантовой аппаратуры | 40 |
| 2.1.1. Универсальное хэширование как способ вычисления имитовставки..... | 40 |
| 2.1.2. Варианты использования хэш-функций для аутентификации | 41 |
| 2.2. Способ взаимодействия квантовой аппаратуры с пользовательскими СЗИ | 52 |
| 2.3. Выводы по главе | 63 |
| 3. Методика распределения общего секрета между узлами сети КРК магистральной топологии | 64 |
| 3.1. Сеть квантового распределения ключей магистральной топологии | 66 |
| 3.2. К вопросу об определении цепочки УКС в сети смешанной топологии | 68 |
| 3.3. Разработка способов распределения общего секрета для конечных узлов | 72 |

| | |
|--|------------|
| 3.3.1. Ожидаемые свойства распределения квантовозащищенных ключей..... | 73 |
| 3.3.2. Разработка способов распределения КЗК..... | 78 |
| 3.4. Классификация способов распределения общего секретного ключа | 92 |
| 3.5. Методика распределения КЗК на пары узлов сети КРК магистральной топологии | 96 |
| 3.6. Выводы по главе | 101 |
| 4. Методика построения сети КРК смешанной топологии | 103 |
| 4.1. Разработка требований к структуре сети КРК | 103 |
| 4.1.1. Требования к уровню потребителей | 108 |
| 4.1.2. Требования к уровню выработки квантовых ключей..... | 109 |
| 4.1.3. Требования к уровню выработки квантовозащищенных ключей | 111 |
| 4.2. Рекомендуемая структура сети КРК | 119 |
| 4.2.1. Порядок распределения КЗК в сети КРК..... | 122 |
| 4.3. Методика построения сети КРК смешанной топологии | 124 |
| 4.4. Выводы по главе | 126 |
| Заключение | 128 |
| Список сокращений и условных обозначений | 131 |
| Список терминов | 132 |
| Литература..... | 134 |
| Список иллюстративного материала | 148 |